Phishing? Cuidado!

Segurança da Informação

Introdução

A informação é um dos principais patrimônios do mundo dos negócios e de todos os indivíduos.

No entanto, por possuir toda essa importância e somado à crescente facilidade de acesso, a informação se tornou um alvo de constantes ameaças no ambiente corporativo e em sua vida pessoal.

Umas das práticas usadas pelos invasores é o phishing.

Para instruir nossos clientes e parceiros, a área de segurança da informação disponibilizou a cartilha sobre phishing.

Nas próximas páginas, saiba o que é, como identificar e como lidar com essa ameaça.

Sumário

O que é um phishing?

Phishing é uma técnica de **engenharia social** usada para enganar usuários!

O **phishing** ocorre por meio do envio de e-mail ou sites maliciosos com objetivo persuadir as pessoas a entregarem suas informações, instalar ou executar programas, baixar documento anexo e clicar em links.

O que pode te prejudicar caso sua identidade seja roubada:

- Cobranças incomuns ou inexplicáveis em suas faturas de cartão de credito;
- Produtos ou serviços que você não contratou;
- Falha no recebimento de contas regulares ou por correio;
- Reprovação inesperada de credito.

O que pode prejudicar uma empresa caso seja roubada suas informações:

- Reputação da empresa;
- Competitividade diante ao mercado;
- Prejuízo financeiro;
- Aspecto legal.

1.

O que é um phishing

Phishing é uma técnica de engenharia social usada para enganar usuários!

2.

Tópicos e temas de mensagens de phishing.

Os temas de mensagens frequentemente usadas nas táticas de phishing.

3.

Como identificar um phishing.

Levantamos ações que devem ser consideradas na identificação de um e-mail de phishing.

4.

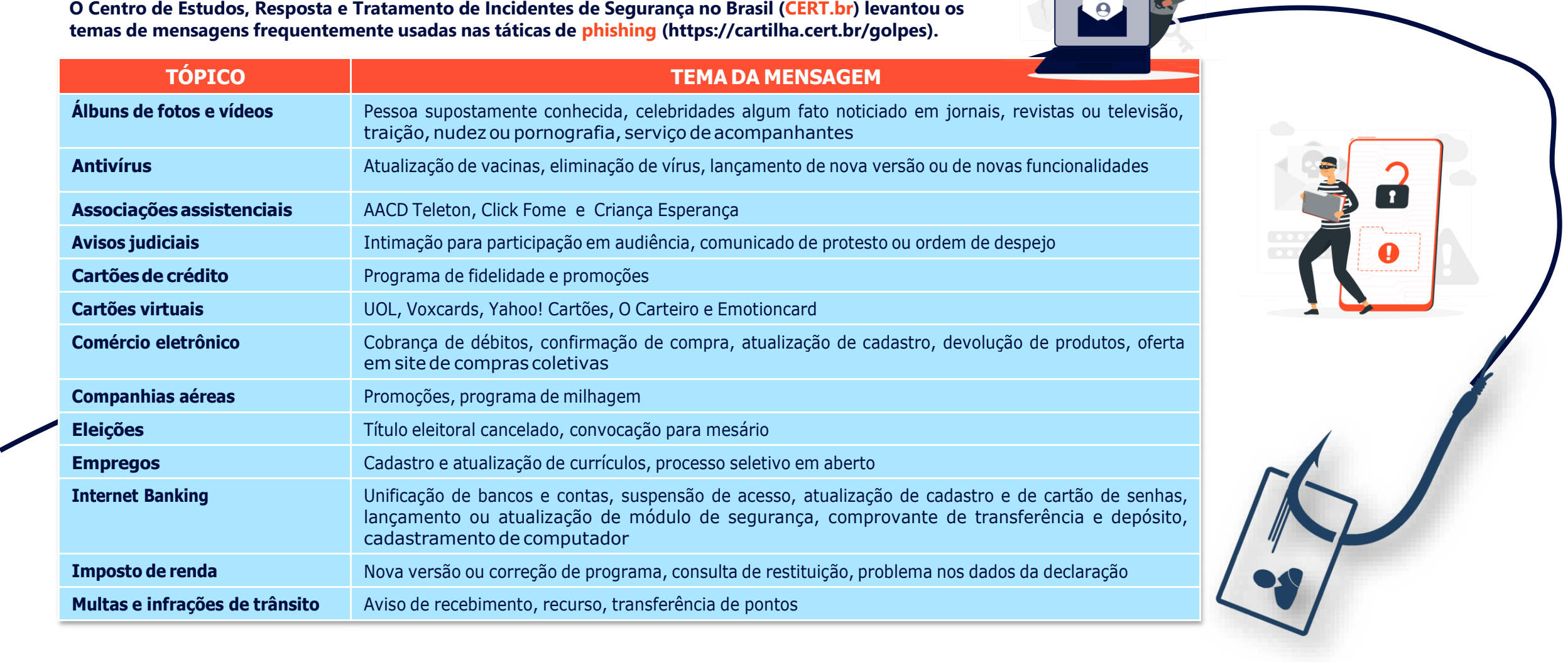
Como lidar com phishing.

Se houver dúvidas quanto a procedência e legitimidade da mensagem que recebeu por e-mail.

Tópicos e temas de mensagens de phishing.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) levantou os temas de mensagens frequentemente usadas nas táticas de phishing (https://cartilha.cert.br/golpes).

TÓPICO	TEMA DA MENSAGEM
Álbuns de fotos e vídeos	Pessoa supostamente conhecida, celebridades algum fato noticiado em jornais, revistas ou televisão, traição, nudez ou pornografia, serviço de acompanhantes
Antivírus	Atualização de vacinas, eliminação de vírus, lançamento de nova versão ou de novas funcionalidades
Associações assistenciais	AACD Teleton, Click Fome e Criança Esperança
Avisos judiciais	Intimação para participação em audiência, comunicado de protesto ou ordem de despejo
Cartões de crédito	Programa de fidelidade e promoções
Cartões virtuais	UOL, Voxcards, Yahoo! Cartões, O Carteiro e Emotioncard
Comércio eletrônico	Cobrança de débitos, confirmação de compra, atualização de cadastro, devolução de produtos, oferta em site de compras coletivas
Companhias aéreas	Promoções, programa de milhagem
Eleições	Título eleitoral cancelado, convocação para mesário
Empregos	Cadastro e atualização de currículos, processo seletivo em aberto
Internet Banking	Unificação de bancos e contas, suspensão de acesso, atualização de cadastro e de cartão de senhas, lançamento ou atualização de módulo de segurança, comprovante de transferência e depósito, cadastramento de computador
Imposto de renda	Nova versão ou correção de programa, consulta de restituição, problema nos dados da declaração
Multas e infrações de trânsito	Aviso de recebimento, recurso, transferência de pontos



Segurança da Informação

Tópicos e temas de mensagens de phishing.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) levantou os temas de mensagens frequentemente usadas nas táticas de phishing (https://cartilha.cert.br/golpes).

TÓPICO	TEMA DA MENSAGEM
Músicas	Canção dedicada por amigos
Notícias e boatos	Fato amplamente noticiado, ataque terrorista, tragédia natural.
Prêmios	Loteria, instituições financeiras.
Programas em geral	Lançamento de nova versão ou de novas funcionalidades
Promoções	Vale-compra, assinatura de jornal e revista, desconto elevado, preço muito reduzido, distribuição gratuita
Propagandas	Produtos, cursos, treinamentos, concursos
Realitys show	Big Brother Brasil, A Fazenda, Ídolos;
Redes sociais	Notificação pendente, convite para participação, aviso sobre foto marcada, permissão para divulgação de foto
Serviços de Correios	Recebimento de telegrama online
Serviços de e-mail	Recadastramento, caixa postal lotada, atualização de banco de dados
Serviços de proteção de crédito	Regularização de débitos, restrição ou pendência financeira
Serviços de telefonia	Recebimento de mensagem, pendência de débito, bloqueio de serviços, detalhamento de fatura, créditos gratuitos

Segurança da Informação

1.

O que é um phishing

Phishing é uma técnica de engenharia social usada para enganar usuários!

2.

Tópicos e temas de mensagens de phishing.

Os temas de mensagens frequentemente usadas nas táticas de phishing.

3.

Como identificar um phishing.

Levantamos ações que devem ser consideradas na identificação de um e-mail de phishing.

4.

Como lidar com phishing.

Se houver dúvidas quanto a procedência e legitimidade da mensagem que recebeu por e-mail.

Segurança da Informação

Como identificar um e-mail de phishing?

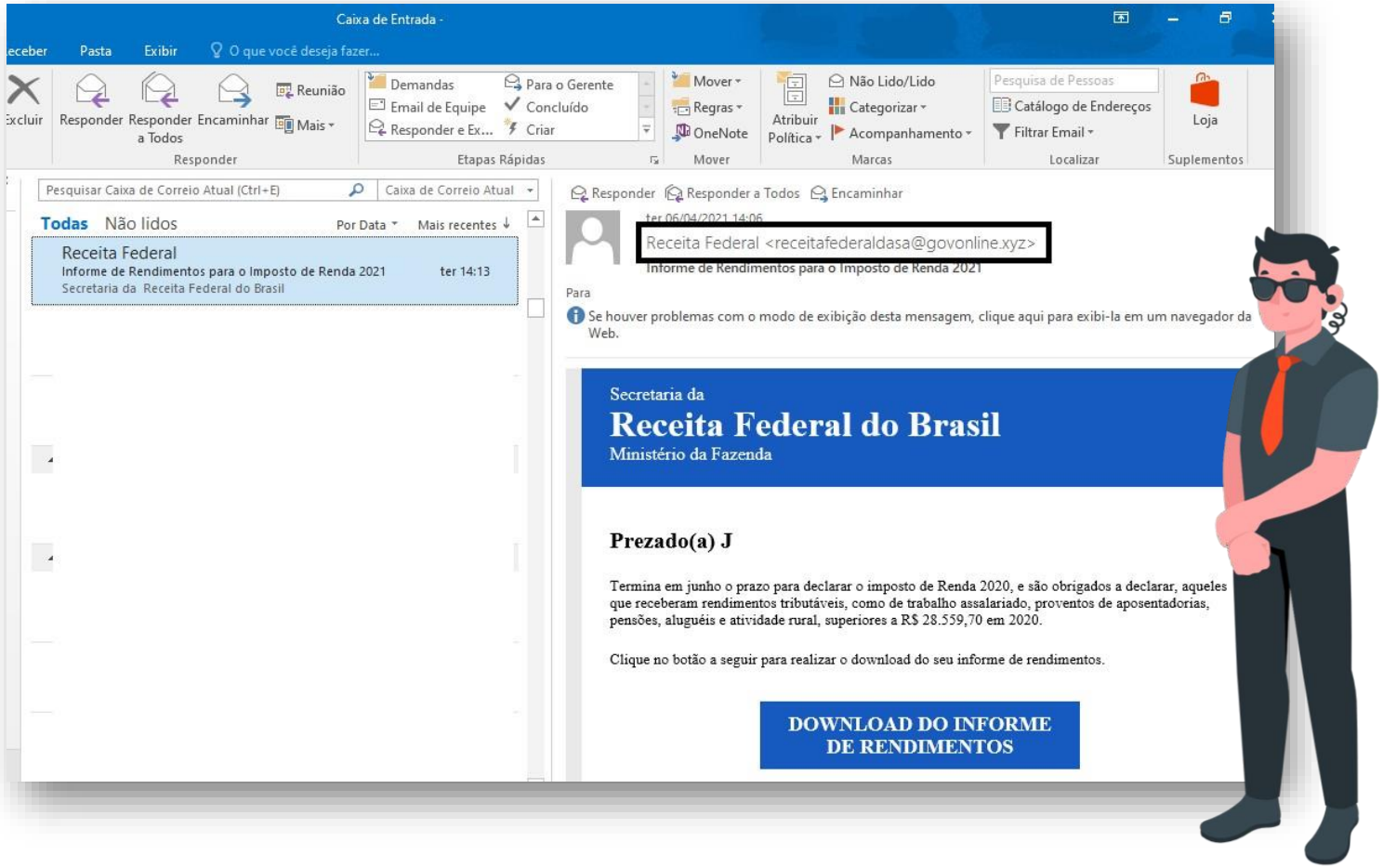
Uma das táticas de **phishing** favoritas é falsificar o nome do remetente.

O nome e o endereço do remetente que aparecem na mensagem podem ser facilmente modificados para mostrar informações falsas.

O Golpista pode usar um endereço de e-mail muito semelhante ao de uma empresa legítima ou órgão fiscalizador.

Verifique o endereço real do remetente e se parecer suspeito, não abra!

Veja o endereço de e-mail do remetente



Segurança da Informação

Como identificar um e-mail de phishing?

Ao receber uma mensagem duvidosa, não acesse links e nem abra os arquivos anexos.

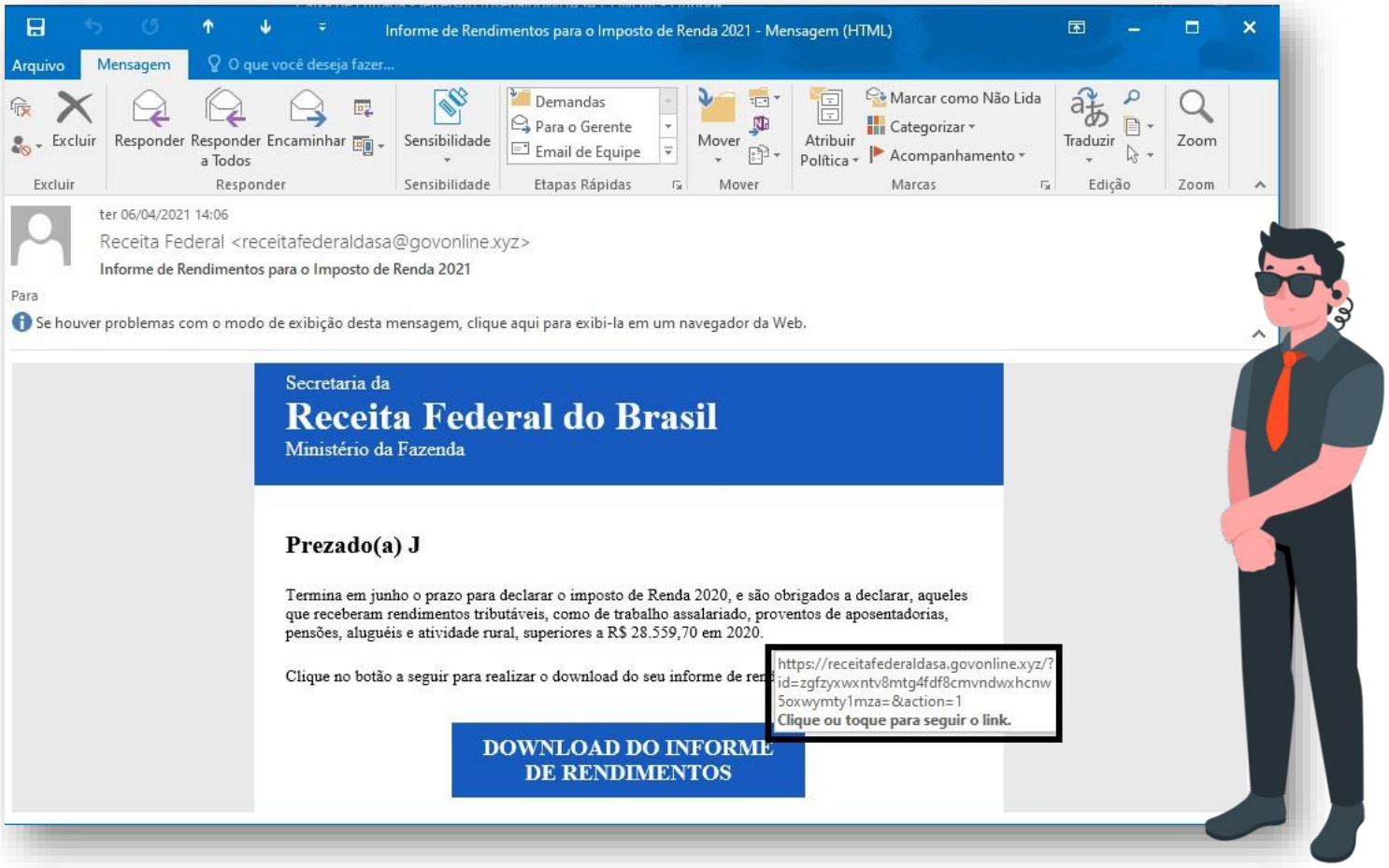
Sempre verifique o link apresentado na mensagem.

Golpistas costumam usar técnicas para ofuscar o link real para o **Phishing**.

Ao posicionar o mouse sobre o link, muitas vezes é possível ver o endereço real da página falsa ou código malicioso.

Se o endereço do link parecer estranho, não clique nele!

Cuidados com links e anexos



Segurança da Informação

Como identificar um e-mail de phishing?

Desconfie de mensagens suspeitas

Empresas legítimas e bancos não enviam mensagens sem o devido cadastro e consentimento do cliente sob hipótese alguma.

Portanto, não acredite em mensagens de origens que você não tenha cadastrado e aprovado anteriormente.

Na dúvida, pegue uma segunda opinião.

Acesse diretamente o site ou os canais oficiais de contato da empresa.

Valide o e-mail no site da instituição remetente

Como identificar um e-mail de phishing?

Desconfie de grandes promoções

Site Falso

Site Real

Por mais tentador que pareça aquela viagem super barata, aquela promoção imperdível ou aquele e-mail cheio de perguntas que promete tirar todas as dúvidas com um simples "clique aqui", desconfie! É aí que se escondem as armadilhas, que colocam você e seus informações em risco.

Como identificar um e-mail de phishing?

Provocar uma sensação de urgência ou medo é uma tática comum.

Fique atento a mensagens que apelem demasiadamente pela sua atenção e que, de alguma forma, o ameacem caso você não execute os procedimentos descritos.

Fique atento a mensagens recebidas em nome de alguma instituição que tentem induzi-lo a fornecer informações, instalar/executar programas ou clicar em links.

Como identificar um e-mail de phishing?

Analise o e-mail criteriosamente:

O e-mail pode ser malicioso contendo um logo convincente, linguagem e um endereço de e-mail aparentemente válido, não significa que é legítimo.

O e-mail pede informações pessoais?

Este é um grande indício que o e-mail é, de fato, malicioso. Empresas e bancos não pedem, sob hipótese alguma, informações pessoais através de e-mails. Não as forneça!

Verifique assinatura do remetente:

Avalie se o e-mail possui assinatura, detalhes sobre o remetente e meios de contato com a empresa.
A ausência dessas informações pode diminuir a legitimidade do e-mail. Empresas sempre fornecem detalhes de contato.

O e-mail possui anexo que não foi solicitado ?

O anexo pode conter código maliciosos, por exemplo um malware que vai dar acesso ao hacker, esse é um dos principais vetores de outros ciberataques.
Por isso, antes de clicar em algum anexo que você tenha dúvidas quanto a procedência e legitimidade valide.

Seja bem criterioso quando se trata de e-mails.

Não acredite em tudo que você vê

Segurança da Informação

1.

O que é um phishing

Phishing é uma técnica de engenharia social usada para enganar usuários!

2.

Tópicos e temas de mensagens de phishing.

Os temas de mensagens frequentemente usadas nas táticas de phishing.

3.

Como identificar um phishing.

Levantamos ações que devem ser consideradas na identificação de um e-mail de phishing.

4.

Como lidar com phishing.

Se houver dúvidas quanto a procedência e legitimidade da mensagem que recebeu por e-mail.

Segurança da Informação

Como lidar com o phishing?

Evite ser uma vítima!

- Fique atendo aos seus e-mails, se eles parecerem minimamente suspeitos, não abra!
- Não revele informações pessoais ou financeiras por e-mail e não responda as solicitações caso suspeite da legitimidade;
- Não envie informações confidenciais pela Internet antes de verificar a segurança de um site:
  - ✓ Preste atenção no endereço do site. Procure endereço que comecem com "https", uma indicação de que os sites são seguros, em vez de "http";
  - ✓ Procure um ícone de cadeado fechado um sinal de que suas informações serão protegidas .
- Se você não tiver certeza que uma solicitação por e-mail é legítima, tente verificá-la entrando em contato diretamente com a empresa. Não use as informações de contato fornecidas no conteúdo do e-mail, em vez disso, abra o navegador e pesquise a empresa ou órgão regulador em site oficial.